Start Small With Data Encryption, FBI and DHS Say

Agency heads say prioritizing what data to encrypt will prevent further roadblocks to accessibility.

James Mersol

Mon, 04/29/2019 - 09:00

Photo credit: MF3d/iStock

Encryption remains one of the most secure ways to protect high-value data. With current technology, encryption keys are effectively unbreakable, unless someone intercepts the key data in what is commonly called a man-in-the-middle attack. However, encryption carries trade-offs; encrypted data travels more slowly and takes time to decrypt irrespective of who is trying to access it. Additionally, agencies are looking forward to implementing end-to-end encryption, which will secure vital data no matter where it is.

Agency leads from the FBI and DHS explained at the 2019 AFCEA Homeland Security Conference last week that encrypting all data, while an appealing idea, will not be successful in application. Even setting aside the time and expense it would take to encrypt existing data, the delays created by transmitting and decrypting data make the process too slow for federal law enforcement, explained FBI Director of Enterprise Services Jeremy Wiltz.

“There’s a lot of overhead that comes with encrypting everything,” he said. “We’re very distributed, so our networks have got to perform — we need data and we need it now.”

Instead, agencies seeking to encrypt their data should identify their priorities and start small, said Vincent Sritapan, who manages the physical and cybersecurity portfolio at the DHS Science and Technology Directorate.

“The first thing I do when I go into an engagement is [tell them], ‘Let’s talk about your most sensitive data and what stuff you’re most afraid of,' and start encrypting those bits first,” he said. Encryption "is going to change some of your organizational workflows ... so start small — crawl, walk, run,” he added.

Organizations need to balance protecting their most sensitive data with understanding the trade-offs for accessibility. “We have to be selective on the kinds of things that we encrypt,” Wiltz agreed.

“It is a risk-based decision,” said Brian Gattoni, chief technical officer for the Cybersecurity and Infrastructure Security Agency (CISA). “There are no one-size-fits-all silver bullets for any of these problems. I tend to have a problem with Zero Trust [as well] — zero is an absolute value. If it’s an absolute approach, there’s probably a challenge there — [I’m looking at] where I best apply something like Zero Trust technology.”

Gattoni recommended that agencies encrypt their high-value core data, but ensure that the push for privacy is not at the cost of delivery of services or the agency’s mission.

Agency leads cited encryption of data in motion as the next major focus that they should look to address. Currently, "data at rest" (data stored on government servers) is encrypted, but travels through networks in its decrypted form, creating a known vulnerability that jeopardizes the integrity of the overall data. The government is looking for solutions to patch the problem.

“Can we transfer data end to end?” said Ron Bewtra, the Department of Justice’s chief technology officer. “Can we watch its integrity and have encryption, and maintain it all the way through our systems? Today we are looking at data at rest — why isn’t it always encrypted? I think we have to continue to work with our industry partners to listen to what is coming up in the emerging world.” Bewtra said he looked forward to coordinating to industry partners to ensure that IT professionals are kept abreast of the latest tools and challenges in encryption.

View printer friendly version

encryption
DHS
DOJ
FBI
cybersecurity
Standard